Configure a Content Security Policy (CSP) header

Content updated: 09/03/2026

This article is designated for administrators.

About

A **Content Security Policy (CSP)** is a standard browser security feature that helps protect a website against cross-site scripting (XSS) and other code-injection attacks. It uses an HTTP header to tell browsers which sources the site is allowed to load resources from, such as scripts, images, styles, fonts, media, and embedded content.

You can configure a CSP header for your Content Hubs or legacy Video Portal site in the **Security module**.

Each organization's policy must reflect the resources, integrations, and customizations used by its site. Kaltura doesn't provide a universal policy because a policy that works for one site may block required resources on another.

Who can use this

Administrators with access to the Configuration Management console can configure the policy.

Your CSP must be tailored to the resources, integrations, and customizations used by your site. Consult your organization’s security or web development team if you need help defining the policy.

Before you start

- Identify the internal and external resources used by your site, including scripts, styles, images, fonts, media, frames, API connections, analytics services, identity providers, integrations, and custom modules.
- Define a CSP that accounts for the resources, integrations, and customizations used by your site. Consult your organization’s security or web development team if you need assistance.
- Test the policy in report-only mode before enforcing it. The system doesn't validate the policy or confirm that required resources can load.

An incomplete or overly restrictive policy may prevent legitimate resources or site functionality from loading.

Understand the CSP fields

The **Security module** provides separate fields for testing and enforcing a policy.

Field	Purpose
`cspHeaderReportOnlyHeader`	Tests a policy on the site without blocking resources. Violations are reported in the browser console.
`adminCspHeaderReportOnlyHeader`	Tests a separate policy for the Configuration Management console without blocking resources.
`cspHeader`	Enforces the policy on the site. This policy also applies to the Configuration Management console when `adminCspHeader` is empty.
`adminCspHeader`	Enforces a separate policy for the Configuration Management console. Use this only when its policy needs to differ from the site's policy.

Use nonce tokens

You can use the following tokens in any of the CSP fields:

- Use the `'nonce-{{scriptNonce}}'` token to generate a random nonce string that is included in script tags.
- Use the `'nonce-{{styleNonce}}'` token to generate a random nonce string that is included in style tags.

Enter only the policy directives in these fields. Don't include the `Content-Security-Policy:` or `Content-Security-Policy-Report-Only:` header name.

For descriptions of all settings in the module, see Security module.

Test the policy

Use report-only mode to identify resources that the proposed policy would block without affecting site functionality.

1. Log in to the **Configuration Management** console.
2. Open the **Security** module.
3. Enter the proposed policy directives in `cspHeaderReportOnlyHeader`.
4. If you plan to use a different policy for the Configuration Management console, enter that proposed policy in `adminCspHeaderReportOnlyHeader`.
5. Click **Save**.

6. Open your browser's developer tools and select the **Console** tab.
7. Test the site's main workflows, including login, search, playback, upload, embedded content, integrations, and any custom features.
8. Review the CSP violation messages in the browser console. Each message identifies the resource that would be blocked and the directive responsible.
9. Work with your security or web development team to update the policy where legitimate resources need to be allowed.
10. Repeat the test until there are no unexpected violations.

Report-only mode helps identify potential problems, but it doesn't enforce the policy or prevent resources from loading.

Apply the policy

After your security or web development team has approved the tested policy:

1. In the **Security** module, copy the tested directives from `cspHeaderReportOnlyHeader` to `cspHeader`.
2. If you tested a separate policy for the Configuration Management console, copy it from `adminCspHeaderReportOnlyHeader` to `adminCspHeader`.
3. Clear the report-only fields.
4. Click **Save**.
5. Test the site and Configuration Management console again to confirm that all required functionality works as expected.

Once `cspHeader` is populated, administrators no longer see the CSP security alert when they log in to the Configuration Management console. Adding a policy only to a report-only field doesn't dismiss the alert.

Update or remove the policy

If the policy blocks a required resource:

1. Open the **Security** module.
2. Review the browser console to identify the blocked resource and the affected directive.
3. Work with your security or web development team to correct the policy. You can also clear the relevant enforced-policy field temporarily to remove that policy.
4. Click **Save**, and then test the affected functionality again.

If the policy prevents you from accessing or using the Configuration Management

console, contact Kaltura Support.